UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/019,827	05/21/2002	Chenghui Luo	Fraunh01.014	8660

25247 7590 09/29/2005

GORDON E NELSON
PATENT ATTORNEY, PC
57 CENTRAL ST
PO BOX 782
ROWLEY, MA 01969

EXAMINER	
SETH, MANAV	

ART UNIT	PAPER NUMBER
2625	

DATE MAILED: 09/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/019,827	LUO ET AL.	
	Examiner	Art Unit	
	Manav Seth	2625	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 May 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-28* is/are rejected.

7)☒ Claim(s) *3* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *5/25/05,6/25/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.1 14

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1 .17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.1 14. Applicant's submission filed on May 25, 2005 has been entered.

Response to Amendment

2. Applicant's amendment under 37 C.F.R. 1.116, filed on March 23, 2005 has been considered and entered in full.

3. Applicant's arguments with respect to respective amended claims on pages 7-13 of the amendment filed May 25, 2005 have been considered but are moot in view of the new grounds of rejection(s).

Claim Objections

4. Claim 3 is objected to for the following informalities:

Claim 3 depends on the canceled Claim 2. It appears that Claim 3 should depend on claim 1.

Furthermore, it is recommended to change the conditional limitations in Claim 1 (use of "may") to positive limitations (e.g., changing, "the watermark may be obtained", to "to obtain the watermark".).

Appropriate correction is required.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Collberg et al., ACM Publication, 1999, "Software Watermarking: Models and Dynamic Embeddings" and further in view of Moskowitz et al., U.S. Patent No. 5,905,800.

Claim 1 recites **"a method of adding a watermark to a sequence of executable instructions to render the sequence authenticable, the method comprising the steps of: receiving the sequence of executable instructions and a key"**. Collberg discloses receiving the sequence of executable instructions and a key (figure 1 (a)-(d); page 311, left column, 2nd paragraph; page 313, right column, section 2; page 315, left column, section 3, paragraph 4))

Claim 1 further recites **"using the key to modify the sequence of executable instructions so that the watermark may be obtained from the modified sequence, the sequence being such that the usefulness of the modified sequence for the sequence's intended purpose is not affected by the modifications made thereto and the watermark representing a watermark value"**. Collberg teaches "Watermarking embeds a secret message into

a cover message" and further discloses software watermarking as "Embed a structure W into a **program P** such that: W can be reliably located and extracting from P even after P has been subjected to code transformation such as translation, optimization and obfuscation; W is stealthy; W has a high data rate; **embedding W into P does not adversely affect the performance of P**; and W has a mathematical property that allows us to argue that its presence in P is the result of deliberate actions" (page 311, left column, abstract) where P being the sequence of executable instructions and W being the watermark which has a mathematical (watermark) value and P+W provides a modified sequence of program P. Collberg further teaches the use of key to add watermark to the object (program) (figures 1(a)-(d) and 2).

Claim 1 further recites **"alteration or absence of the watermark value being used when the sequence is authenticate to determine whether the sequence is authentic"**. Collberg clearly teaches "W has a mathematical property that allows us to argue that its presence in P is the result of deliberate actions" (page 311, left column, abstract). Collberg's. As it is well known that adding watermarks will provide copyright security to the programs and how susceptible a program is to be getting copied depends on how good is the watermark and therefore it apparently is the watermark value as disclosed by Collberg ("W has a mathematical property that allows us to argue that its presence in P is the result of deliberate actions") that provides the authenticity of the program or the sequence. Collberg further teaches "**the application O (program) is run with a predetermined input sequence I= I_1....I_k which makes the application enter a state which represents the watermark**" (page 315, left column, 4th para., section 3) and further under the same section 3 further provides that if the watermark authentication fails, the code will display a copyright message or an unexpected image on the screen (page 315, left column, 6th para) and further teaches "

figure 2 (4) shows a watermark being embedded within the state of a program O as it is being run with a particular input I. **The watermark is extracted by examining the current values held in O's variables, after the end of the input sequence has been reached"** (page 315, left column, 8th para.). Collberg further teaches "**the watermark is extracted by monitoring some properties of the address trace and/or the sequence of operators executed"** (page 316, left column, 1st para) and further teaches "some watermarks that are written in the program text or static data are susceptible to attacks that increase the static size of the code" (page 317, left column, 4th para). It is clear from above disclosures by Collberg that it's the watermark value that provides the authentication of the sequence and the alteration or absence of watermark value would fail the authenticity of the program. Collberg, further adding emphasis, teaches that if the watermark is tampered, it fails the program (page 314, right column, last para.). Collberg does not provide very clear teachings and for the sake of better clarity that it's the watermark value that determines the authenticity of the program, examiner cites Moskowitz. Moskowitz as from the title discloses a method and system for digital watermarking. Moskowitz discloses general facts of watermarking by teaching **"To make a watermark virtually impossible to find without permissive use of the key, it's encoding is dependent upon a randomly generated sequence of binary 1s and 0s, which act as the authorization key. Whoever possesses this key can access the watermark"** (col. 3, lines 25-32). Moskowitz further discloses **"Digital watermark can be encoded with random or pseudo-random keys, which act as secret maps for locating the watermarks. These keys make it impossible for a party without the key to find the watermark – in addition, the encoding method can be enhanced to force a party to cause damage to a watermarked data stream when trying to erase a random-key watermark"** (col. 1, lines 40-50) and further discloses "this would make it possible for parties possessing a decoder to verify the

presence of valid watermarks in a data stream, without accessing the contents of the watermark. It would also be possible to scan or search archives for files containing watermarked content, and to verify the validity of the presence of such files in an archive, **by means of the information contained in the watermarks**" (col. 1, lines 62 through col. 2, lines 1-5). Moskowitz further discloses "such a system ... provides a way for the user to input constraints on the application of the digital watermark key, and provides a way to store this information with a random or pseudo random key sequence which is also generated to apply to a content signal. Such a system would also be more readily adaptable by current techniques to master content with personal computers and authoring/editing software. It would also enable individuals to monitor their copyrights with decoders **to authenticate individual purchases**, filter possible problematic and unpaid copyrightable materials in archive, and provide for a more generally disturbed approach to the monitoring and protection of copyrights in the digital domain" (col. 2, lines 60-68 through col. 3, lines 1-5). Therefore, examiner asserts, that it would have been obvious for one of ordinary skill in the art at the time of invention was made to use combined teachings of Collberg and Moskowitz as discussed before, to use watermark values to authenticate the sequence, as the appropriate watermark key can only access the watermark for further processing, and thus preventing the access of sequence of executable instructions after alteration or absence of watermark of the watermark value.

Claim 3 recites "The method set forth in Claim 1 wherein the step of modifying the sequence includes the steps of: using the key to determine locations in the key including modification locations at which the sequence is to be modified and modifying the sequence at the modification locations such that the locations specified by the key represents the watermark value

whereby the watermark value may be obtained from the modification locations". As discussed in the rejection of claim 1, both Collberg and Moskowitz teaches the use of key which represents the watermark values. Moskowitz further teaches "in effect, the key is a map describing where in the content signal the information signal is hidden" (col. 3, lines 30-32).

Claim 4 has been similarly analyzed and rejected as per claims 1 and 3.

Claim 5 recites "the method set forth in claim 4 wherein: the instructions at the locations specified by the key represents values of digits of the watermark values". As discussed before in the rejection of claim 1, Moskowitz discloses general facts of watermarking by teaching "To make a watermark virtually impossible to find without permissive use of the key, it's encoding is dependent upon a randomly generated sequence of **binary 1s and 0s**, which act as the authorization key. Whoever possesses this key can access the watermark" (col. 3, lines 25-32). Also, the use of watermark mathematical value is disclosed by Collberg, as discussed before.

Claims 6 and 7 have been similarly analyzed and rejected as per claims 1-5.

Claim 8 recites "the method set forth in claim 1 wherein: the modified sequence of executable instructions is modified such that when the modified sequence of executable instructions is executed, execution state is produced which has a property that depends on the key. Where the watermark value is a description of execution state from the modified sequence". As discussed in the rejection of claim 1, Collberg teaches "**the application O (program) is run with a predetermined input sequence I= I_1....I_k which makes the application enter a state which represents the**

watermark" (page 315, left column, 4th para., section 3) and further teaches " figure 2 (4) shows a watermark being embedded within the state (global, heap, and stack data, etc.) of a program O as it is being run with a particular input I. **The watermark is extracted by examining the current values held in O's variables, after the end of the input sequence has been reached**" (page 315, left column, 8th para.). All other arguments applicable to rejection of claims 1-5 are also applicable to claim 8.

Claim 9 recites "the method set forth in claim 9 wherein: the execution state is stack depth graph". As discussed before Collberg teaches "Figure 2 (4) shows a watermark being embedded within the state (global, heap, and **stack data**, etc.) of a program O as it is being run with a particular input I. **The watermark is extracted by examining the current values held in O's variables, after the end of the input sequence has been reached**" (page 315, left column, 8th para.). Collberg further teaches stack depth graph in figure 3.

Claims 10-14 have been anticipated by Collberg in figures 2, 3 and 5 and further support can be found on (page 315, right column; page 316; page 317, section 5, more emphasis added on sections 5.1 and 5.3).

Claims 15-17 have been similarly analyzed and rejected as per claims 1-8.

Claim 18 has been similarly analyzed and rejected as per the arguments used in the rejection claims 1-8.

7. Claims 19-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Collberg et al., ACM Publication, 1999, "Software Watermarking: Models and Dynamic Embeddings", further in view of Moskowitz et al., U.S. Patent No. 5,905,800, and further in view of Low et al., "A taxonomy of Obfuscating transformations".

Claim 19 recites "the method of authenticating set forth in claim 18, the method further comprising the step of: receiving another watermark value; and in the step of using alteration or absence of the watermark value determine whether the received sequence is authentic, the watermark value is compared to the other watermark value". As discussed in the rejection of claims 1-8, both Collberg and Moskowitz teach the receiving of watermark value which further is used to authenticate the program instruction sequence. Collberg does not teach the method comparing one watermark value to the other watermark value to authenticate the program instruction sequence. However, examiner asserts that comparing two watermark value to authenticate is very well known in the art and Moskowitz provides the teachings by disclosing **"Human-assisted watermarking would provide an improvement over the art by providing flexibility as to where information signals would be inserted into content while giving the content creator the ability to check all subsequent copies without the requirement of a single original or master copy for comparison. Thus the present invention provides for a system where all necessary information is contained within the watermark itself"** (col. 4, lines 42-50). The above disclosure as by Moskowitz shows that Moskowitz does not use comparison method but shows an improvement over comparison method, however, these teachings provide the evidence of comparison method being known as prior art. However, in order to provide more support for the well-known comparison method, which is not used by Collberg and Moskowitz to authenticate, examiner cites Low.

Low, similarly as Collberg and Moskowitz, teaches "technical protection of software secrets" and further teaches automatic code obfuscation, which is the most viable method for preventing reverse engineering (Abstract, 2nd para; page 3, right column, 3rd para). Code obfuscation works on the same path as watermarking which adds the code to the program and Low provides the support of this adding the code to the program in (page 7, left column, 5th paragraph) where it discloses **"if program P and P' are identical except that P' contains more of property q than P, then P' is more complex than P. Given such a statement, we can attempt to construct a transformation which adds more of the q-property to a program, knowing that this is likely to increase its obscurity"** and further provides the support on page 23 in right column of section 9 by disclosing **"An obfuscated application really consists of two programs merged into one : a real program which performs a useful task and a bogus program which computes useless information. The sole purpose of the bogus program is to confuse potential reverse engineers by hiding the real program behind irrelevant code. The opaque predicate is the main device the obfucator has at its disposal to prevent the bogus inner program from being identified and removed"**. Low further provides the teachings of statistical analysis which can be used for evaluation (authentication) and further provides the support on comparing two obfuscated programs for evaluation (authentication) purposes (page 25, section 9.5). Therefore, it would have been obvious for one of ordinary skill in the art at the time of invention was made to use the teachings of Low in the combined invention of Collberg and Moskowitz because all the references are directed to control the software piracy and copyright protection and Moskowitz as discussed before provides the improvement over comparison method which is further used by Low but additionally using the comparison method as described by Low would provides an additional method to authenticate the software authentication to protect software piracy and copyright.

Claim 20 has been similarly analyzed and rejected as per claims 1-8 and 18-19.

Claim 21 has been similarly analyzed and rejected as per claims 18-19 and 1-8.

Claim 22 has been similarly analyzed and rejected as per claims 21, 18-19 and 1-8

Claim 23 has been similarly analyzed and rejected as per claims 22 and 1-9.

Claims 24-28 has been similarly analyzed and rejected as per claims 18-22 and 1-17.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Saito, U.S. Patent No. 6,002,772, discloses a data management system which uses electronic watermark technique to prevent piracy or leakage of data content.
- Houser et al., U.S. Patent No. 5,606,609, discloses electronic document verification system and method.
- Leighton, U.S. Patent No. 5,664,018, discloses a watermarking procedure which resilient to collusion attacks.
- Moskowitz et al., U.S. Patent No. 5,822,432, discloses method for human-assisted random key generation and application for digital watermark system.

- Linnartz et al., U.S. Patent No. 6,209,092, discloses a method and system for transferring content information and supplemental information relatinf thereto which further provides the use of watermarking.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Manav Seth whose telephone number is (571) 272-7456. The examiner can normally be reached on Monday to Friday from 8:30 am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bhavesh Mehta, can be reached on (571) 272-7453. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

BHAVESH M. MEHTA
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600

Manav Seth
Art Unit 2625
March 8, 2005